

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization International Bureau



(43) International Publication Date
29 April 2004 (29.04.2004)

PCT

(10) International Publication Number
WO 2004/036396 A1

- (51) International Patent Classification⁷: **G06F 1/00**, 17/60, 19/00 // 155/00, 161/00
- (74) Agent: TANDBERGS PATENTKONTOR AS; Boks 7085, N-0306 Oslo (NO).
- (21) International Application Number: PCT/NO2002/000376
- (22) International Filing Date: 17 October 2002 (17.10.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant (for all designated States except US): CONAX AS [NO/NO]; Fred Olsens Gate 6, N-0152 Oslo (NO).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): LARSEN, Øystein [NO/NO]; Hesteskøen 25, N-1407 Vinterbro (NO). NICOLAYSEN, Wictor [NO/NO]; Hurdalsgata 2, N-0655 Oslo (NO). BLOM, Harald [NO/NO]; Larsbråtvæien 4, N-0674 Oslo (NO). SANDVIK, Vidar [NO/NO]; Oppegårdsgata 6B, N-0196 Oslo (NO). STOKKE, Frode [NO/NO]; Monradsgate 1E, N-0577 Oslo (NO).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

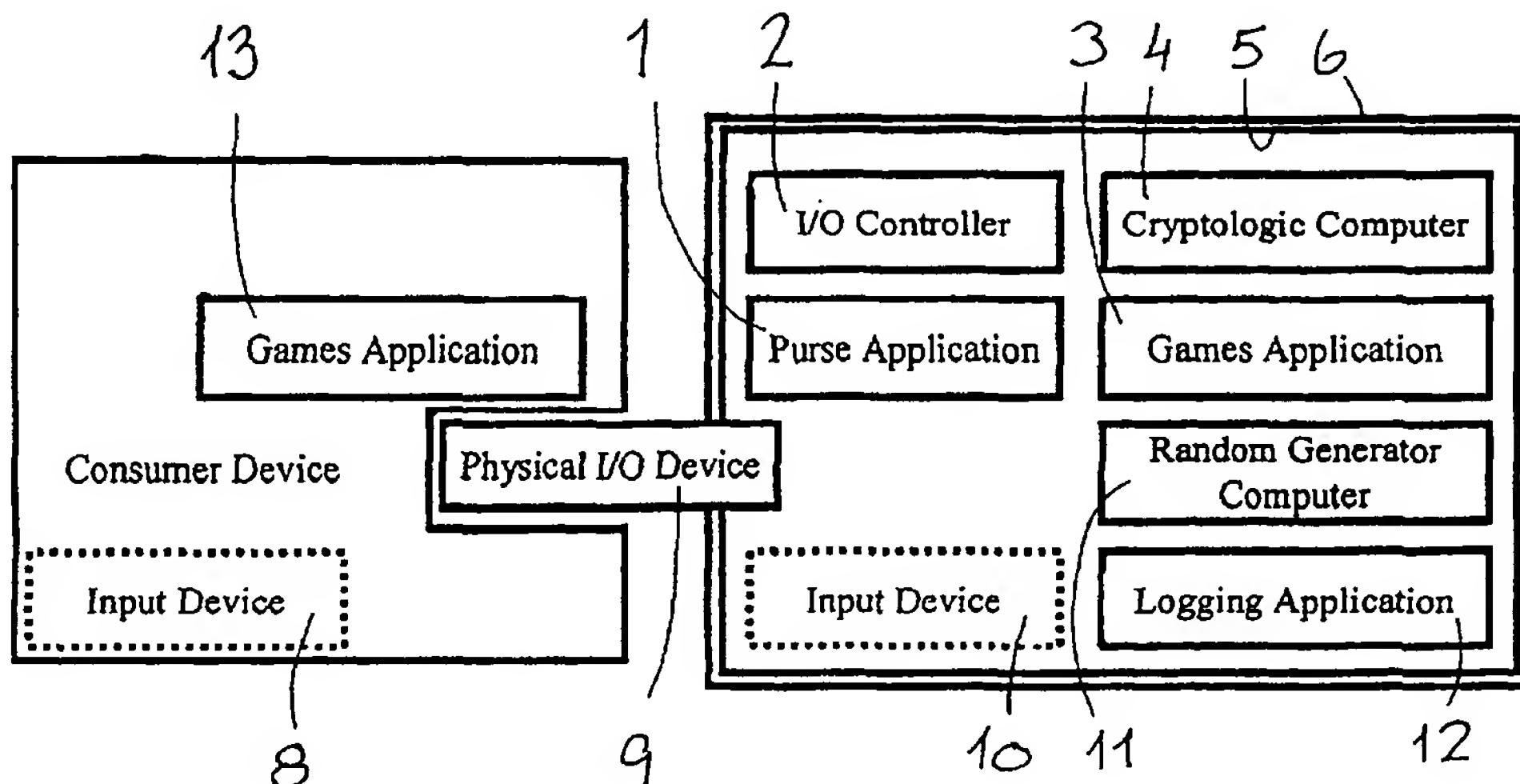
Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE OFFLINE BETTING DEVICE

p



WO 2004/036396 A1

(57) Abstract: A method and a secure offline betting device for playing games offered by a betting operator offline and away from the premises of the betting operator, the device thereby comprising a purse application (1), an I/O controller (2), a games application (3, 13), a cryptologic application (4), a physical I/O device (9), a random generator application (11) and a logging application (12) all encapsulated in a tamperproof physical enclosure (5).

83206-SS

Secure Offline Betting Device

5 The present invention is related to a secure offline betting device for electronic betting on games offered by a betting operator, outside of the premises of the betting operator, without being online connected to the betting operator.

By using cryptographic techniques (e.g. Public Key Cryptography, Digital Signature, and Public Key Infrastructure) it is possible today to ensure the integrity of
10 data and applications and set specific access privileges to authorised users. Several different means for user identification exist (e.g. PIN code based methods, devices with biometric sensors and more). Several technologies exist for electronic betting systems operated on a computer system in a secure data centre or in a vending machine operated under surveillance. Some betting systems also provide online remote access from a,
15 cellular phone, PDA, digital TV set-top box or other device. There are today no device that provides these techniques and functionality integrated and combined in a tamper-proof manner to obtain a secure offline betting device.

In many situations it is important and necessary for a betting operator to offer
10 offline electronic betting away from the premises of the betting operator or its reseller.
Such situations occur for example in areas where legislation disallows online betting transactions or online payment transactions when used in combination with betting. Users
15 in such areas may be able to play games in their homes, or other places, away from the premises of the betting operator or its resellers, using a tamper proof device that can be loaded/unloaded with money and containing a gaming engine. The offline betting may be
20 performed on a consumer device such as any computer, cellular phone, PDA, digital TV set-top box, or other device.

To comply with such a requirement a gaming device must be able to i) hold a purse that can be loaded and unloaded at a betting operator or its reseller, deducted when
25 a bet is done and topped if a winning, ii) perform the logics of a game (e.g. blackjack, poker, bingo, slot etc), iii) log transactions, iv) generate random numbers, v) encrypt applications and data, vi) hold a set of access privileges, like the gaming operator may load and unload the purse, the user does not have access to change the purse, the user has only access to the gaming engine and vii) only let an authorised operator and authorised user access the betting device.

30 The above requirements are fulfilled by the secure offline betting device according to the present invention as defined by the features stated in the patent claims. The secure offline device combines and integrates the above-mentioned techniques into a tamper-proof device. This ensures the integrity of the games with winnings and losses as well as only letting an authorised user play games.

With the secure offline mobile betting device according to the invention, a user can be authenticated towards a betting operator i.e. he is allowed to use the secure offline betting device.

The invention will ensure that only an authorised betting operator may load and unload money to/from the betting device. Furthermore it will be ensured that only an authorised betting operator may unload the log from the betting device and that only an authorised user may play the games on the betting device.

The invention also will ensure non-repudiation, i.e. the user of the betting device cannot deny having played games and thereby emptied the purse in the betting device.

According to the invention it further is ensured that, based on signed log information analysis, the winnings on the betting device is within a statistical acceptable pattern, the authorised betting operator is allowed to exchange money hold in the purse with cash

Still according to the invention, logs are gathered from the entire betting device population to analyse winnings and losses to verify that the payout percentage is within the defined range set for the various games

By providing encryption and digital signatures, access to functions in the betting device is only available to an authorised betting operator and an authorised player. The identification may be a PIN code, biometrics etc. If the identification is legal, the betting device will provide access to functions. If not, the betting device will respond that the identification is invalid. If wrong identification is provided more than a predefined number of times, the betting device will be blocked.

The enclosed drawing shows a structural block diagram

The secure offline betting device consists of the following functional blocks: A purse application, a game application, a random generator application, a logging application, a cryptologic application, an I/O controller, a physical I/O device and optionally an input device. All these sub-devices are encapsulated in a tamperproof physical enclosure, or wrapping.

The purse application holds the money in the secure offline betting device. Money, or tokens, in the purse can be used to play a game or exchanged for cash at a betting operator. The purse application may be loaded at a betting operator or if the user wins a game. The purse may be a running on a shared/dedicated smart card microchip or some other computational device able to perform general computations.

The games application may contain logics for games (e.g. slot, black jack, poker, bingo, roulette, lotto etc.). The game application may be fully or partially running on a shared/dedicated smart card microchip or some other computational device able to perform general computations or be running fully or partially in the consumer device.

The random generator is an application either running on a shared/dedicated smart card microchip or some other computational device able to perform general computations.

5 The logging application logs transactions when they are performed. The log data may be un-signed, or signed for security reasons. The logging application may be a running on a shared/dedicated smart card microchip or some other computational device able to perform general computations.

10 The cryptologic application may be running on a shared or dedicated smart card microchip or some other computational device able to perform cryptographic and security functions as well as general computations.

The I/O controller is either dedicated hardware and/or driver software to (necessary) support the communication towards the physical I/O device.

The physical I/O device may be any standard connector (plug) or devices, e.g. USB, ISO 7816 smart card interface, PCMCIA and others.

Patent Claims

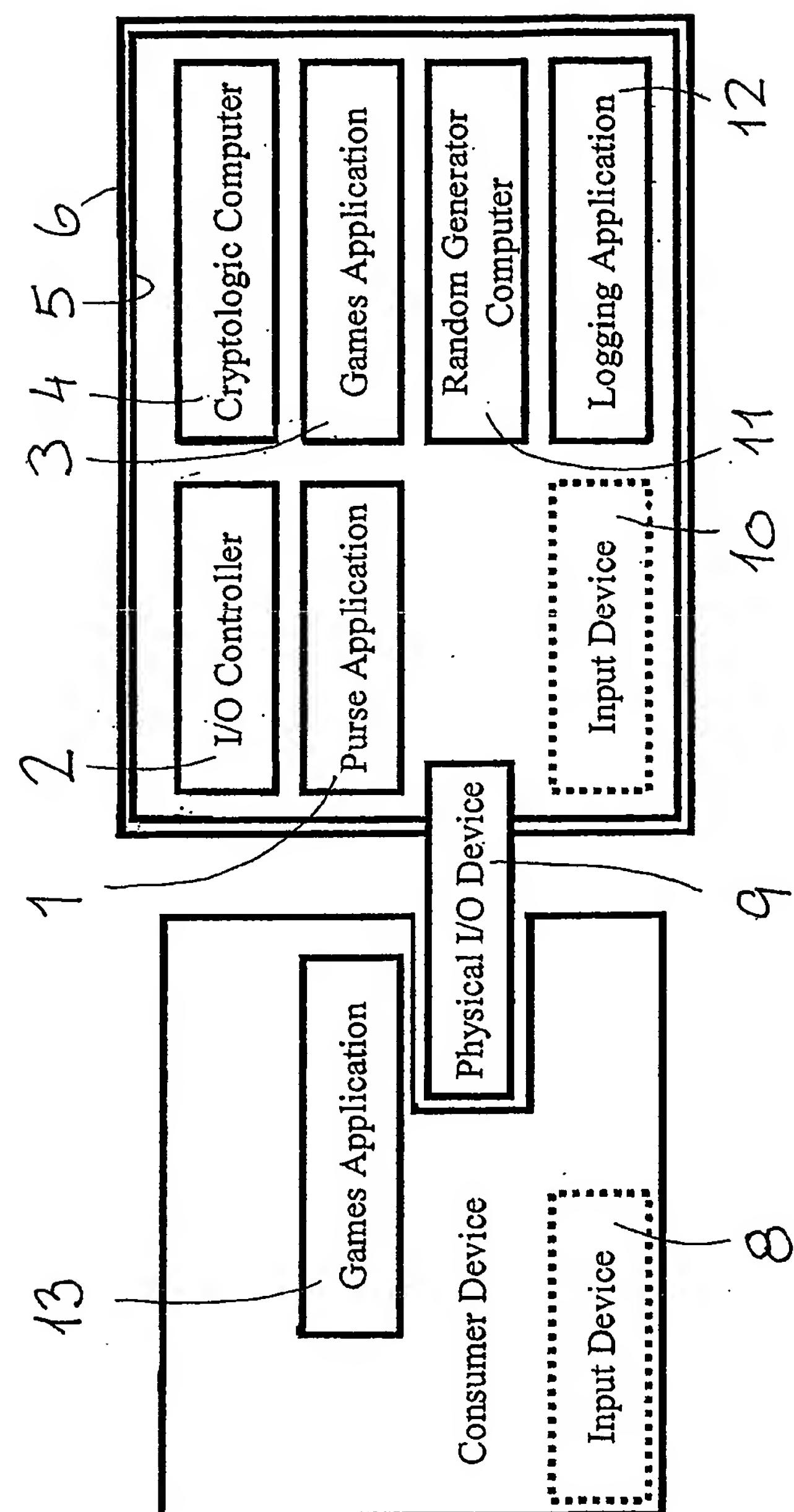
5

1. A secure offline betting device for playing games offered by a betting operator offline and away from the premises of the betting operator, **characterized in** the device comprising a purse application (1), an I/O controller (2), a games application (3, 13), a cryptologic application (4), a physical I/O device (9), a random generator application (11) and a logging application (12) all encapsulated in a tamperproof physical enclosure (5).

10 2. A method for providing offline betting on games offered by a betting operator, **characterized in** (i) an authorised betting operator may load and unload the betting device with money or tokens, (ii) an authorised betting operator may load and unload the betting device with entitlements i.e. authorisations for actual games, (iii) an 15 authorised betting operator may unload the transaction log from the betting device, (iv) an authorised user may access information regarding money or tokens held by the betting device, (v) an authorised user may run games and thereby increase or decrease the money or tokens held by the betting device, whereby the game may be a slot, blackjack, poker, bingo or any other game.

20

1/1



INTERNATIONAL SEARCH REPORT

International application No.

PCT/NO 02/00376

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 1/00, G06F 17/60, G06F 19/00 // G06F 155:00, G06F 161:00
 According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F, G07F, A63F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9600950 A1 (WALKER ASSET MANAGEMENT LTD PARTNERSHIP), 11 January 1996 (11.01.96), page 3, line 1 - page 13, line 32, abstract --	1,2
X	US 6234898 B1 (BELAMANT, S.C.P. ET AL), 22 May 2001 (22.05.01), abstract --	1,2
A	US 5276312 A (MCCARTHY, R.S.), 4 January 1994 (04.01.94), abstract --	1,2
A	US 5781723 A (YEE, B. ET AL), 14 July 1998 (14.07.98), column 1, line 26 - column 2, line 3, abstract --	1,2

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:	
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search	Date of mailing of the international search report
7 May 2003	16-05-2003
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Åsa Viken /LR Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.

PCT/NO 02/00376

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6347738 B1 (CREVELT, D.E. ET AL), 19 February 2002 (19.02.02), abstract ---	1,2

INTERNATIONAL SEARCH REPORT

Information on patent family members

29/03/03

International application No.

PCT/NO 02/00376

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9600950 A1	11/01/96	AU 698557 B AU 2953195 A AU 8025494 A AU 8701898 A BE 1010001 A BR 9405271 A CA 2137498 A CN 1122032 A DE 4437277 A DK 11395 A FI 950950 A FR 2717283 A,B GB 2287342 A,B GB 9425080 D GR 1002724 B GR 95100048 A HU 71560 A HU 9500288 D IE 950162 A IL 111758 A IL 114359 D IT 1281324 B IT MI950164 A JP 7255950 A LU 88582 A MC 2402 A NL 9402220 A NO 950746 A OA 9971 A PL 307582 A PT 101671 A SE 9500437 A TR 28375 A US 6527638 B WO 9524689 A ZA 9505451 A	29/10/98 25/01/96 21/09/95 12/11/98 04/11/97 17/10/95 12/09/95 08/05/96 14/09/95 12/09/95 12/09/95 15/09/95 13/09/95 00/00/00 03/07/97 30/11/95 28/12/95 00/00/00 20/09/95 05/04/98 00/00/00 18/02/98 11/09/95 09/10/95 18/03/96 26/07/96 02/10/95 12/09/95 11/12/95 18/09/95 12/09/95 12/09/95 23/05/96 04/03/03 14/09/95 13/02/96
US 6234898 B1	22/05/01	AP 918 A AP 9801263 D AU 711945 B AU 7632596 A EP 0939939 A GB 9602869 D IL 124564 A NZ 322548 A CA 2238351 A CN 1207817 A RU 2170947 C WO 9719428 A ZA 9609762 A	29/12/00 00/00/00 28/10/99 11/06/97 08/09/99 00/00/00 10/02/02 28/10/99 29/05/97 10/02/99 20/07/01 29/05/97 24/04/98

INTERNATIONAL SEARCH REPORT

Information on patent family members

29/03/03

International application No.

PCT/NO 02/00376

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US 5276312 A	04/01/94	AU 9153591 A		08/07/92
		BR 9107145 A		19/04/94
		MX 174091 B		20/04/94
		MX 9102483 A		01/06/92
		OA 9782 A		15/04/94
		WO 9210806 A		25/06/92
<hr/>		NONE		
US 5781723 A	14/07/98	AU 721733 B		13/07/00
		AU 1913497 A		06/11/97
		CA 2202689 A		29/10/97
		EP 0805424 A		05/11/97
		US 5902983 A		11/05/99
		ZA 9703623 A		25/11/97